Firewall

Presented By:

Manav Raj

What is Firewall?

A firewall is a system designed to prevent unauthorized access to or from a private network.

We can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets

Types of Firewall

There are 3 types of Firewall

PACKET FILTER FIREWALL

Packet Filter Firewall controls the network access by analyzing the outgoing and incoming packets.
Packet filtering technique is suitable for small networks but gets complex when implemented to larger networks.

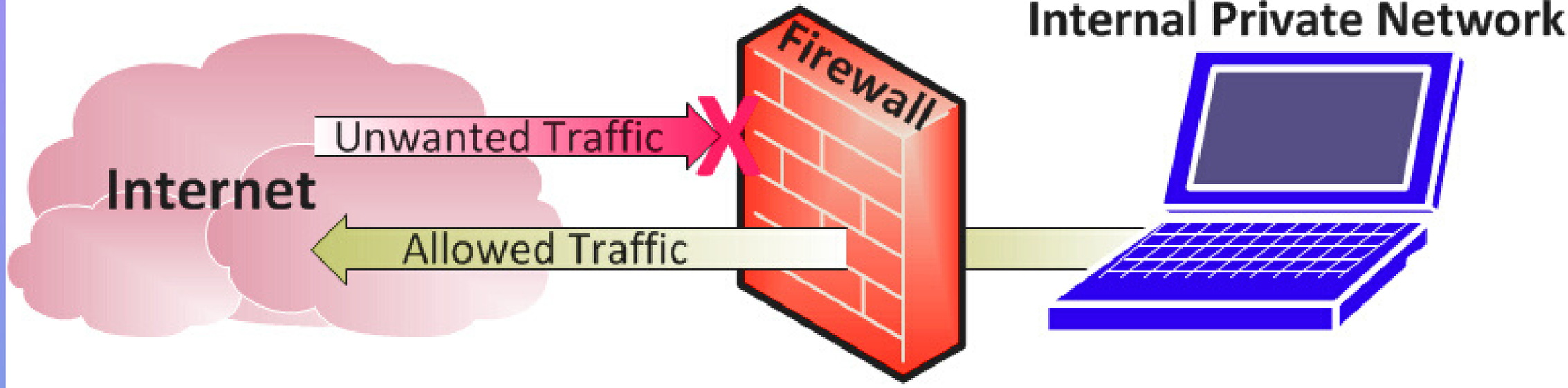
STATEFUL INSPECTION

Stateful Packet Inspection (SPI), which is also sometimes called dynamic packet filtering, is a powerful firewall architecture which examines traffic streams from end to end

PROXY SERVER FIREWALLS

roxy Server Firewalls are the most secured type of firewalls that effectively protect the network resources by filtering messages at the application layer. Proxy firewalls mask your IP address and limit traffic types.

Computer Firewalls



Where firewalls are typically located?

FIREWALLS CAN BE PLACED ANYWHERE ON A NETWORK BUT ARE MOST COMMONLY LOCATED BETWEEN THESE COMPONENTS:

Console and the Application Server
Application Server and the agents
Agent Manager and IBM Security Host Protection agent
Agent Manager IBM Security Server Protection for Windows agents
Event Collector and agents
Application Server and the Internet
X-Press Update Server and the Internet (IBM Security Download Center)

How Firewalls Work?

WHAT FIREWALL SOFTWARE DOES?

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.